DNS Query Traffic Increase on Caching DNS Resolvers

DNS-OARC Workshop
October 13-14, 2010
Denver

Hiroaki Iinou and Minoru Zushi（NTT Communications, OCN）
Haruhiko Nishida and Kazumichi Sato（NTT Laboratories）

Outline

1. Query Traffic Increase on OCN DNS Caching Servers
   - Introduction to OCN
   - Query Trends on OCN DNS Caching Servers
   - Query Increase Analysis

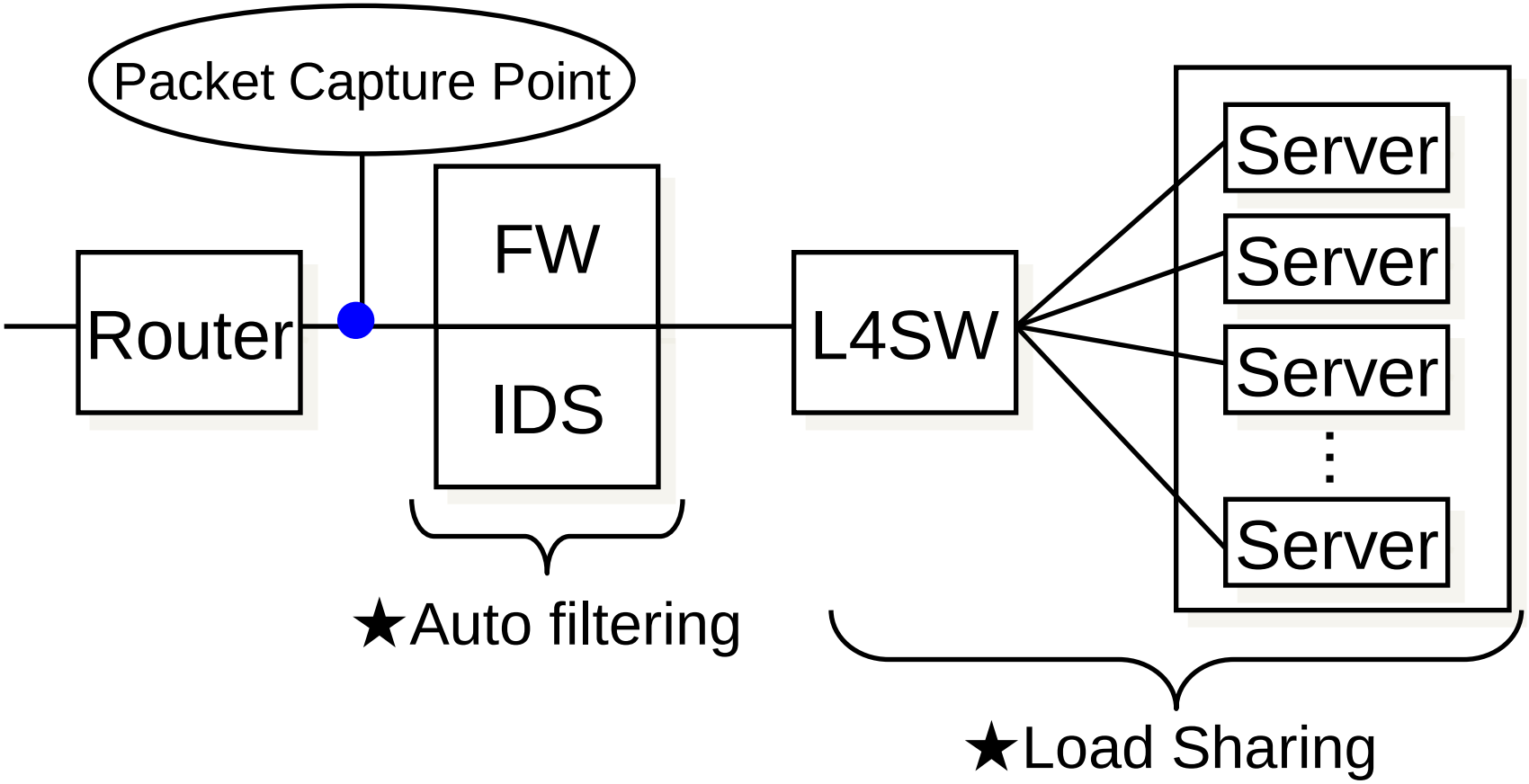
2. Topic of near future
   - Influence of DNSSEC

Introduction to OCN

- **Background of OCN (AS4713)**
  - Largest ISP in JAPAN
  - 8 million customers

- **DNS operation**
  - 6 billion queries/day (70,000 queries/sec)
  - 150 DNS servers
    - 50 name servers / 100 caching servers
  - 2 kinds of DNS application
    - BIND9 / Vantio (Vantio has 6 times the performance compared to BIND)

OCN Cache DNS Structure

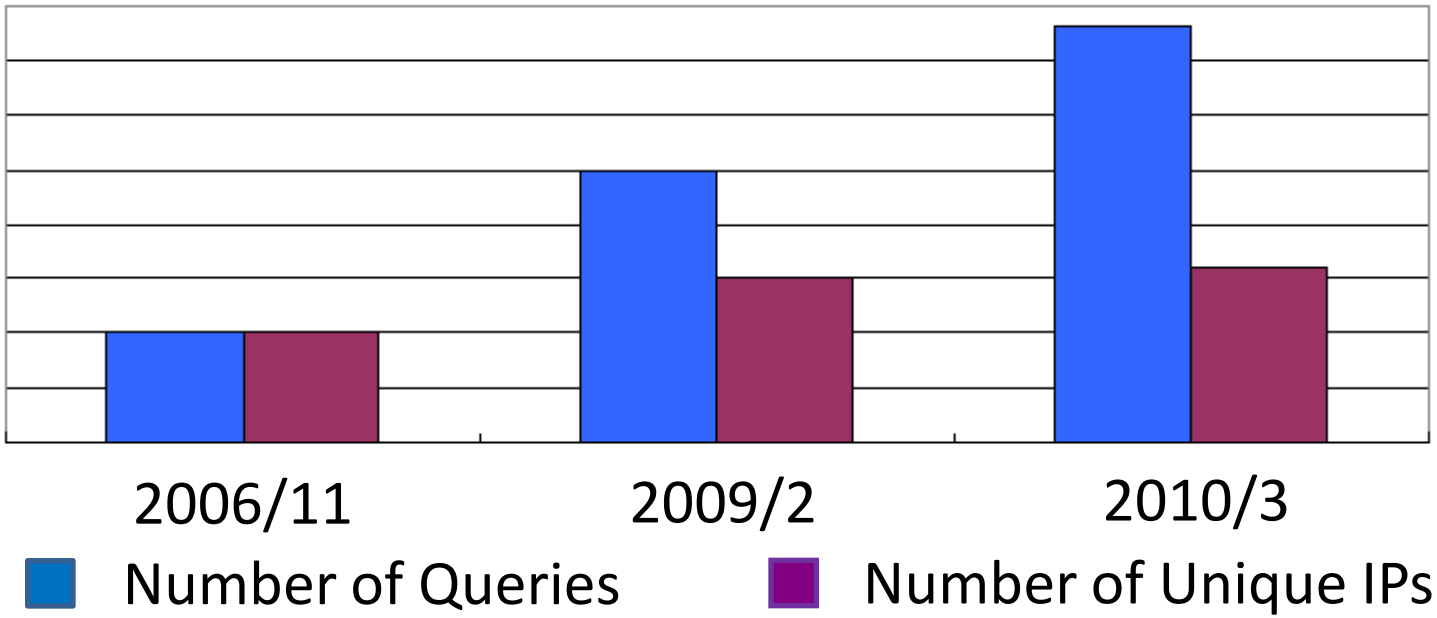


DNS Query Traffic Transition

■ Number of queries and unique IP addresses per day at 3 random points in 3 different years shown below.

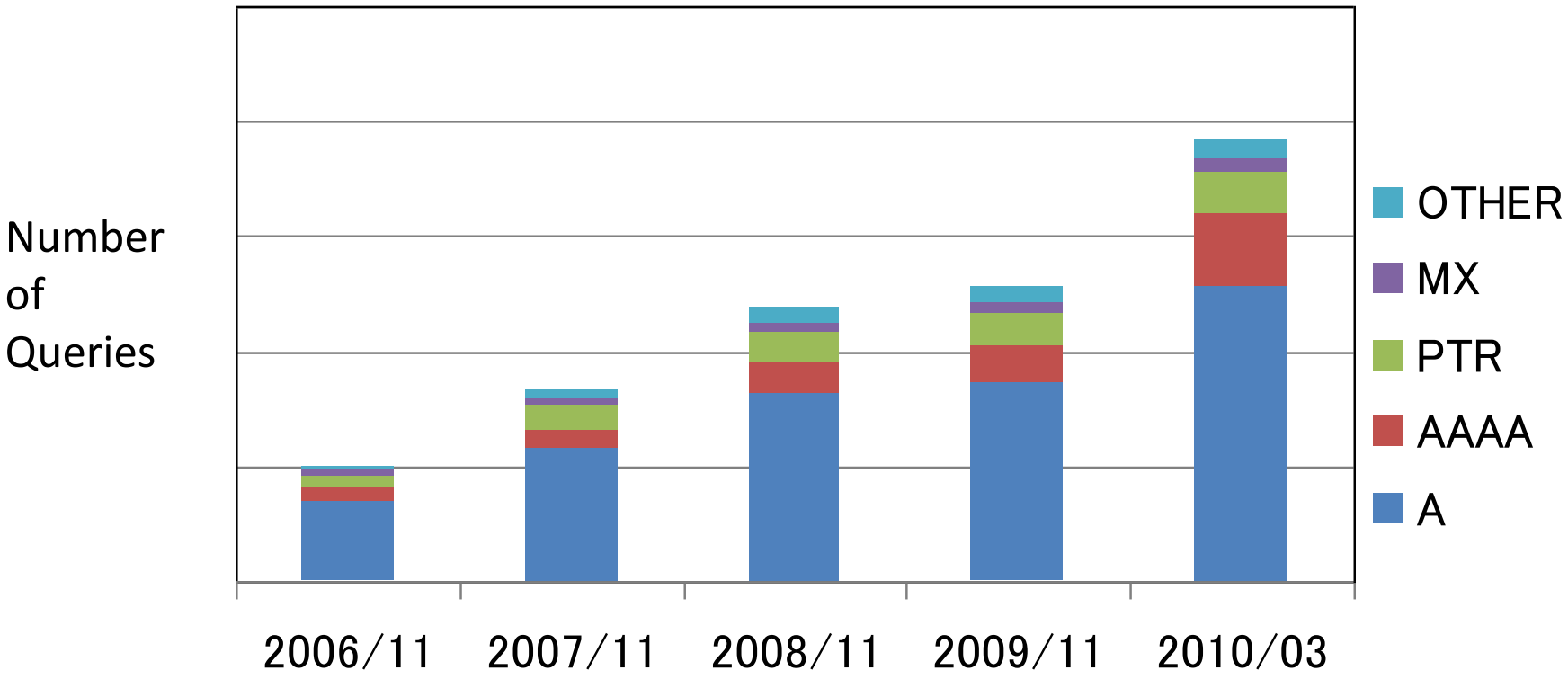
■ Both number of queries and number of unique IPs increased. However, increase in number of queries much greater than that in number of unique IPs.

⇒ **Number of queries by each user increased**



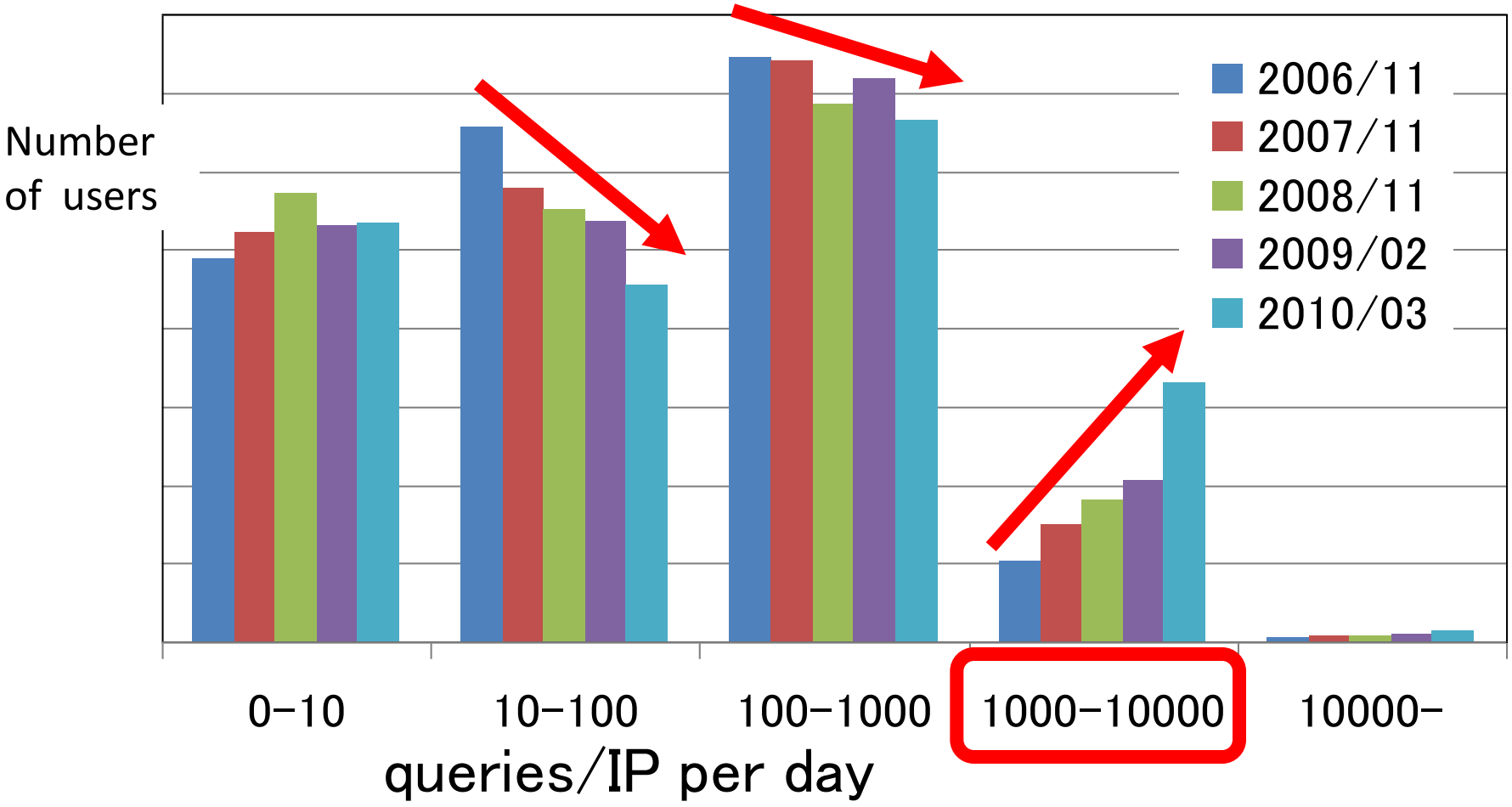
What Type of Query?

- In particular, increase of A/AAAA is remarkable.
  （about 1.5 times compared with 2009/11）



Transition for Query for Each IP

■ IPs that transmit over 1,000 to 10,000 queries per day specifically grew as shown.



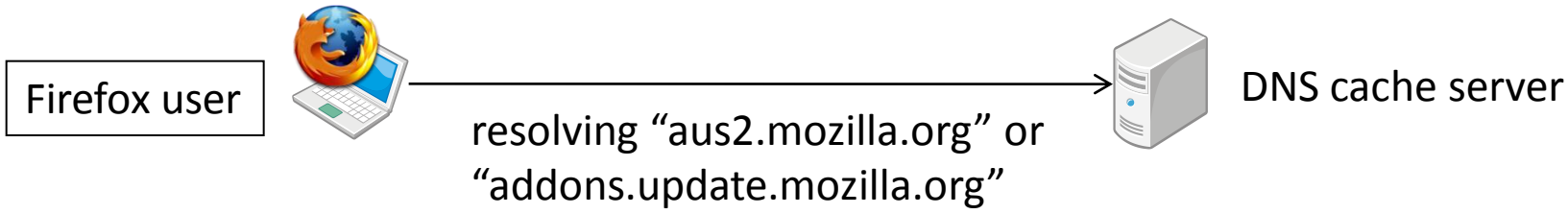
Query Increase Analysis

Cause of Increase of Heavy Users

- Number of heavy users in Mar. 2010 increased compared with number in Feb. 2009
- What is cause of increase?
  - DNS prefetch function was implemented in Firefox in June 2009
  - Found that number of Firefox users as heavy users increased
  - Suspect that DNS prefetch function caused increase in number of heavy users
- Validate our hypothesis
  - Compare number of queries sent by Firefox users in Mar. 2010 with that in Feb. 2009

Extract Firefox Users

- Find hosts that resolve domain names of Firefox or addons update server
  - "aus2.mozilla.org" or "addons.update.mozilla.org"
- Assume found hosts are Firefox users
  - Firefox users may resolve above domain names



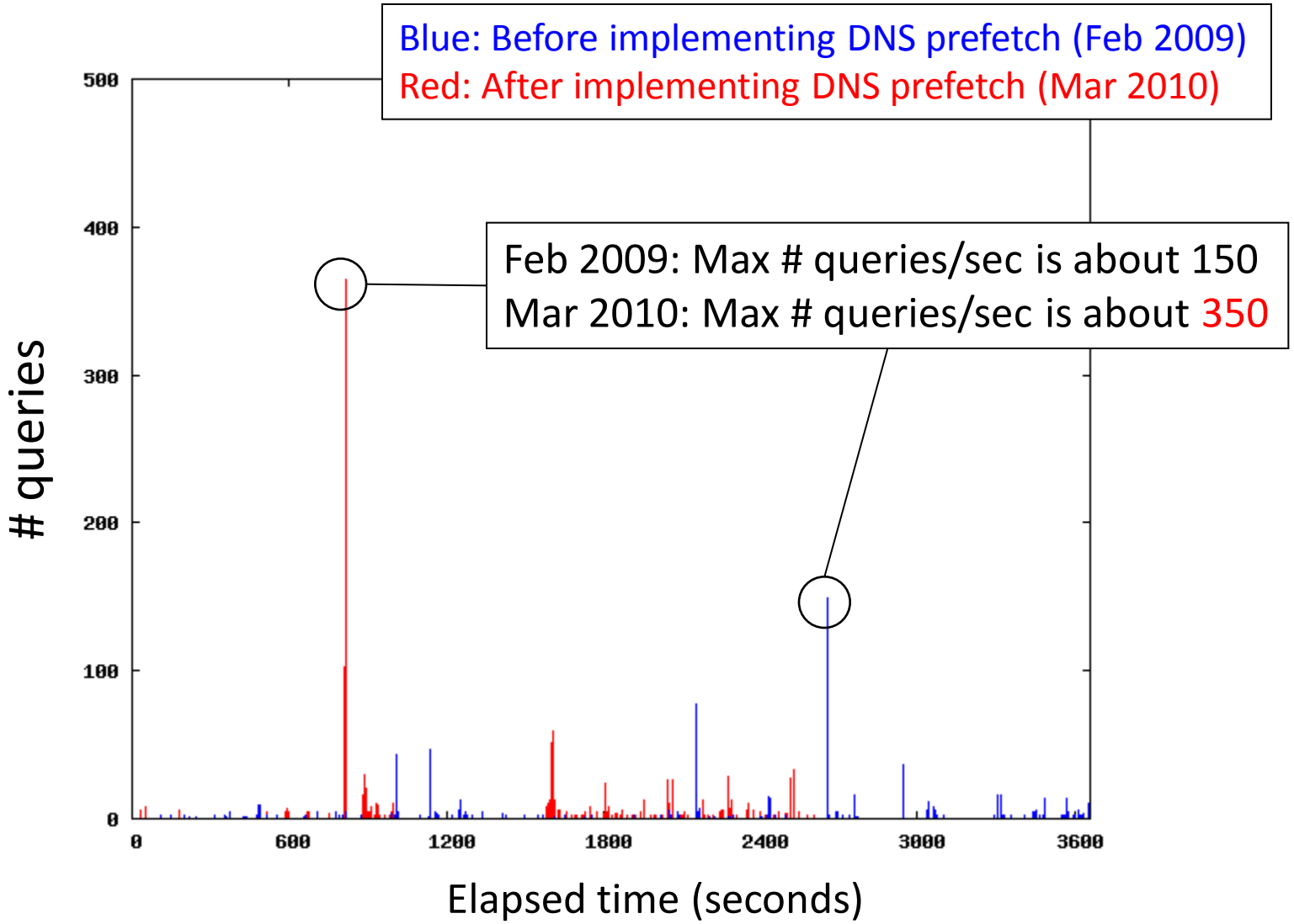
Note: We cannot extract all Firefox users. In addition, we may extract users that do not use Firefox.

Number of Firefox Users in Heavy Users

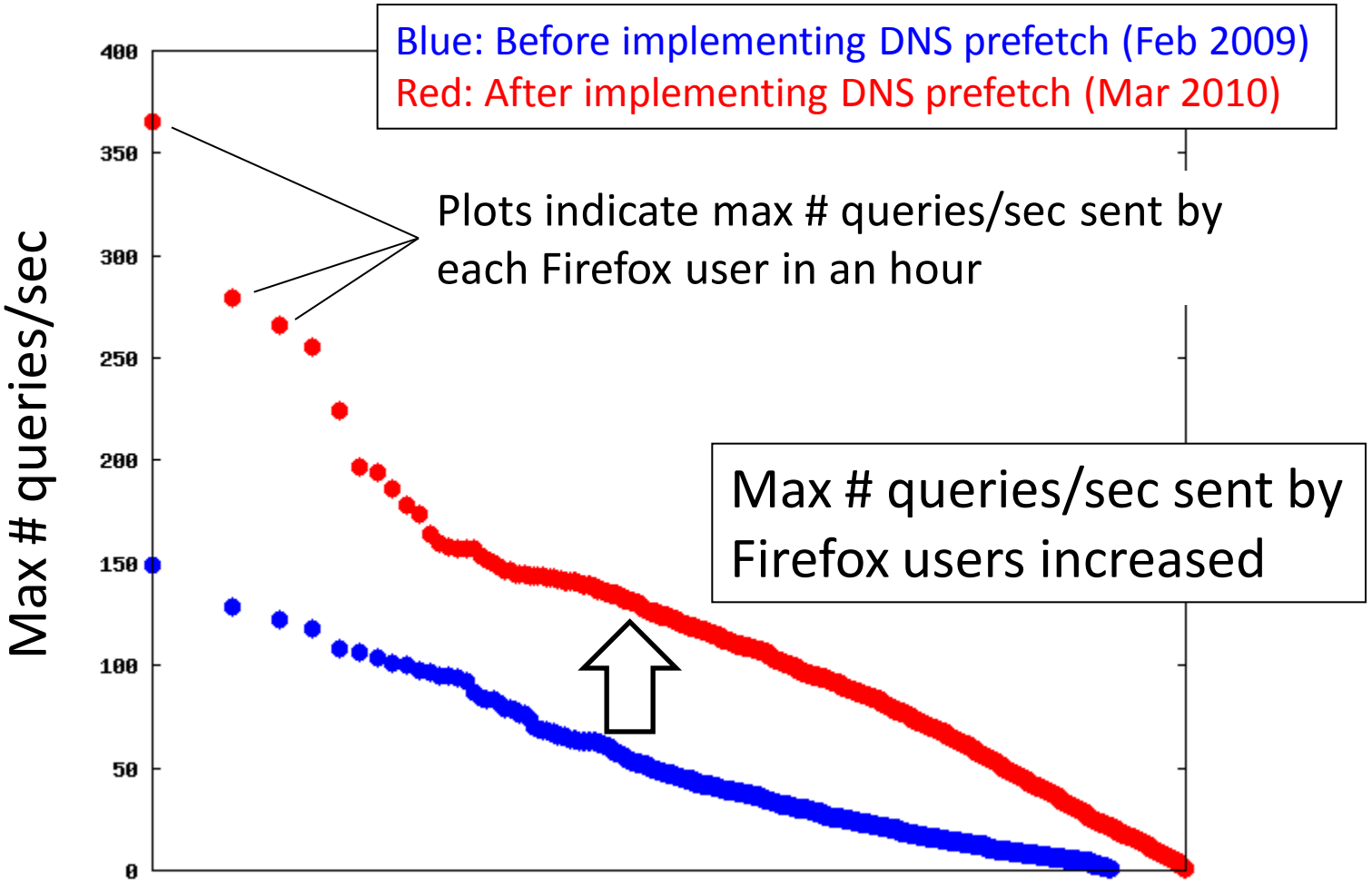
- Inspected number of Firefox users in heavy users
  - Find heavy hosts that send more than 100 queries in one second
  - Extract Firefox hosts in heavy users as heavy Firefox users
  - Compare number of hosts in Mar. 2010 with Feb. 2009
- Comparison Results
  - Heavy users have increased by 4 times in a year
  - Heavy Firefox users have increased by 28 times in a year

	Feb 2009	Mar 2010
#Heavy Firefox users	0.02	0.55
#Heavy users	1	4

Number of Queries Sent by Top Query Rate Firefox Users



Number of Queries per Second Sent by Firefox Users



Discussion

- Number of queries sent by Firefox users increased after DNS prefetch function was implemented
  - Feb. 2009: Max number of queries was about 150
  - Mar. 2010: Max number of queries was about 350
  - DNS prefetch function may have caused increase in heavy users
- Difficult to distinguish whether queries sent by heavy users are bogus or not
  - So far, queries sent by heavy users have almost all been bogus

- If query rate is limited by stateful firewall, queries sent by Firefox users may be blocked
- NAT box state table may be full
- If DNS prefetch function is implemented in Internet Explorer, DNS cache server load may increase

- Our suggestion
  - Require decreasing prefetch query rate of vendors

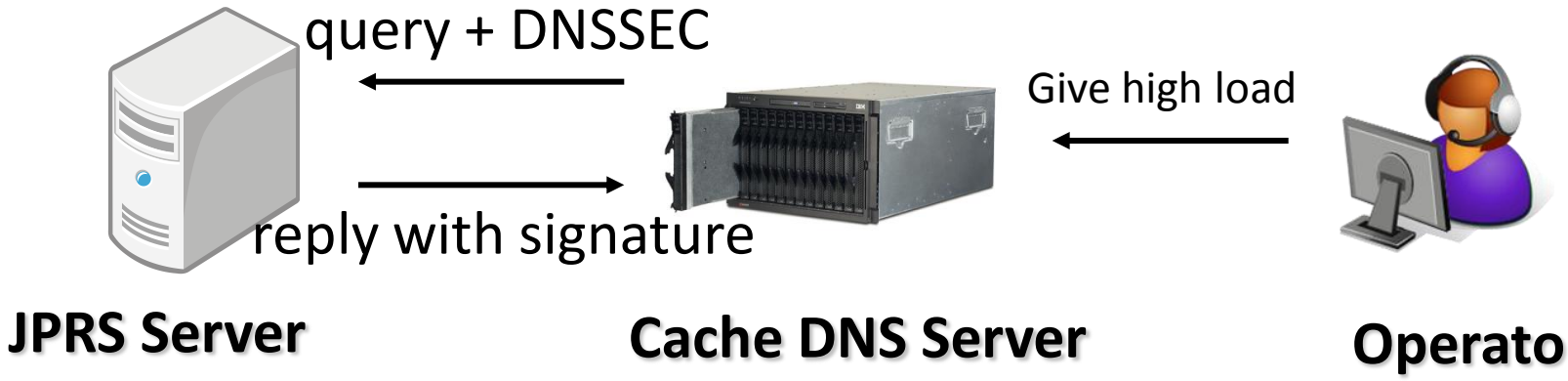
Topic of near future

Influence of DNSSEC

May 2009: We started a joint experiment with JPRS.

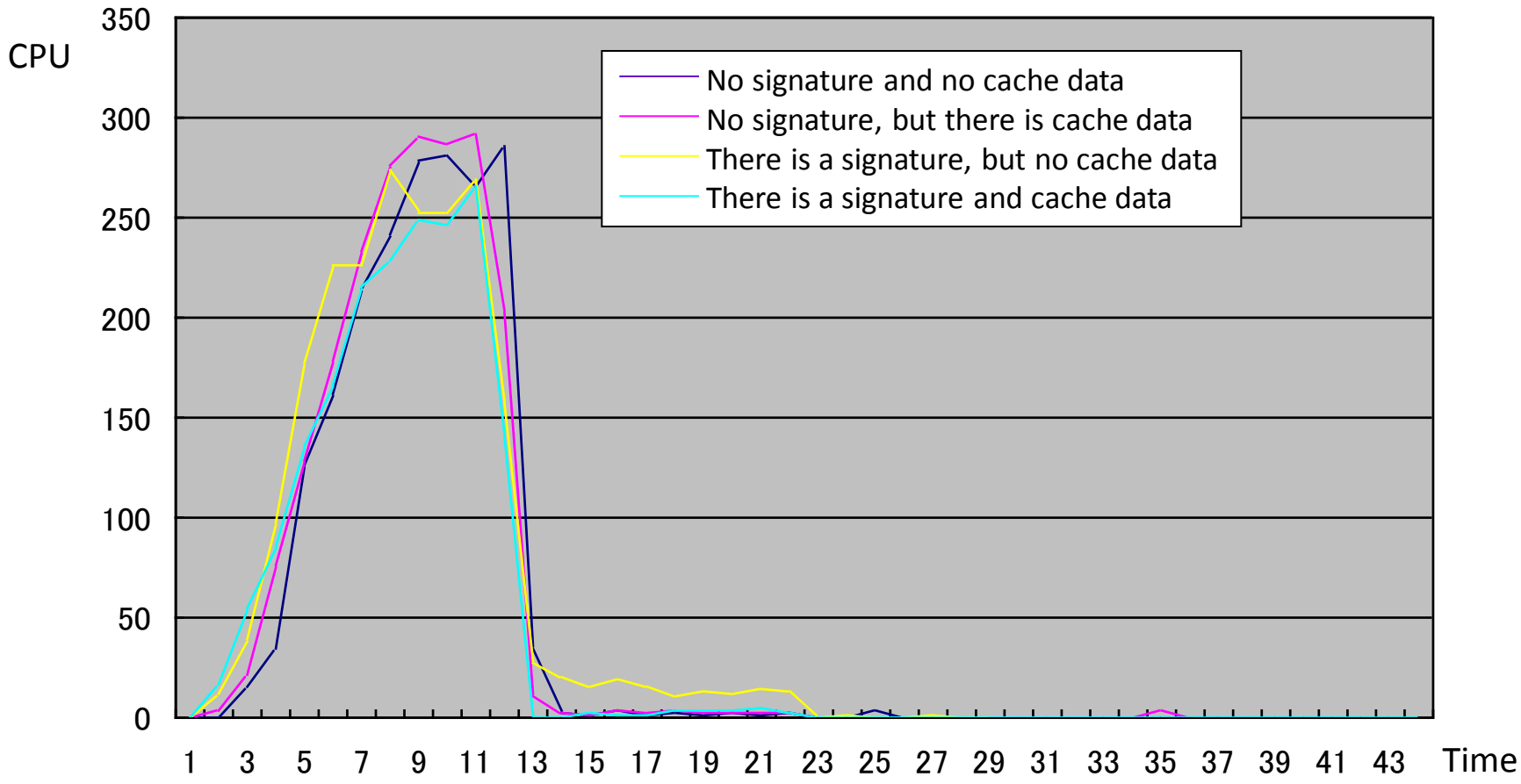
(JPRS manages .jp ccTLD)

1. Investigated cache DNS server procedure in order to support DNSSEC.
2. Investigated impact of load that DNSSEC gave to a cache DNS server.



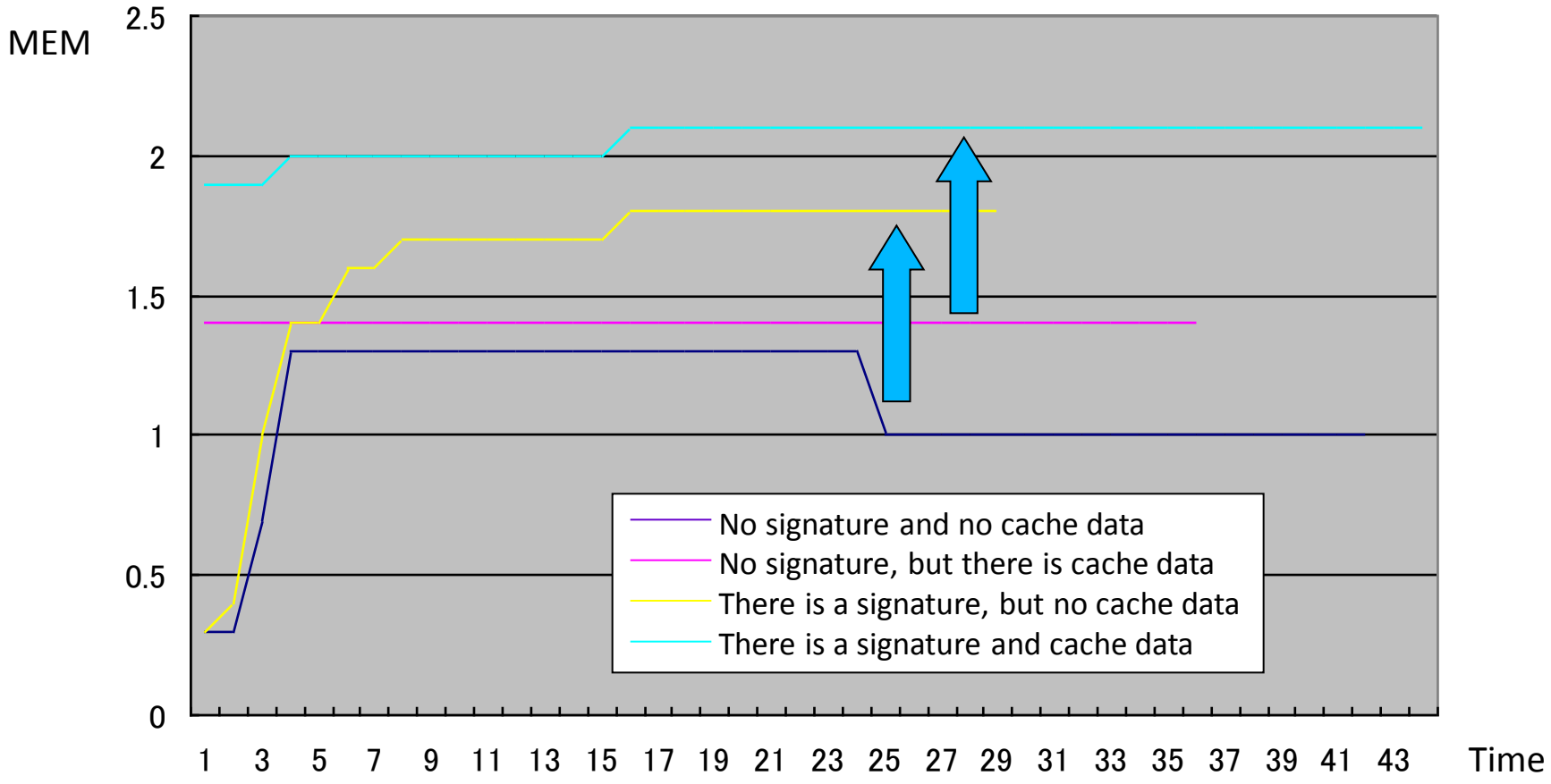
Results of experiment （CPU）

CPU Usage: No big change



Results of experiment (Memory)

Memory Usage: **About a 2 times increase**



Summary of DNSSEC experiment

1. Data size accumulated in cache increases

- Increase of memory usage occurs in particular

- Bands of network also increase

2. Necessary to ensure high precision data by several experiments

3. Necessary to consider impact in network devices (load balancer, firewall, etc.)